

バイオメトリクス認証

2012年6月7日 10:30~12:00

才所 敏明
(株)IT企画

toshiaki.saisho@advanced-it.co.jp

1

< 本日の内容 > バイオメトリクス認証

- (1) バイオメトリクス認証とは
- (2) 本人確認における
バイオメトリクス認証の位置づけ
- (3) 各種バイオメトリクス認証方式の概要紹介
- (4) バイオメトリクス認証プロセス
- (5) バイオメトリクス認証の
ナショナルセキュリティへの応用
- (6) バイオメトリクス認証応用の将来

2

(1)

バイオメトリクス認証とは

- (1) バイオメトリクス認証とは
- (2) 本人確認における
バイオメトリクス認証の位置づけ
- (3) 各種バイオメトリクス認証方式の概要紹介
- (4) バイオメトリクス認証プロセス
- (5) バイオメトリクス認証の
ナショナルセキュリティへの応用
- (6) バイオメトリクス認証応用の将来

3

人が持つ生体特徴により、 本人確認を行う認証方式

人は

- * 顔を見て、その人だとわかるように
- * 電話で声を聞いて、その人だとわかるように

あらかじめ知っている人の生体特徴(顔、声など)と
どの程度似ているかにより、その人と判断

バイオメトリクス認証も、
あらかじめその人の生体特徴を登録しておき、
その場に居る人の生体特徴と突きあわせ、
その似ている度合いにより、その人であると判断

4

マンションやオフィスへの応用(1)



声紋認証
AmiVoice Guard



指紋認証

出典: <http://www.advanced-media.co.jp/newsrelease/newsrelease.cgi?detail=20070510152943>

出典: <http://www.n-axis.co.jp/cms/0/>

5

マンションやオフィスへの応用(2)



指静脈認証

出典: <http://premium.mikicorp.co.jp/s/2005/special/21702.html>



手のひら静脈認証

出典: <http://pr.fujitsu.com/jp/news/2005/08/18.html>

6

ATMへの応用



指静脈認証

出典: <http://www.hitachiyoron.com/2005/01/highlight13.html>



手のひら静脈認証

出典: <http://japan.cnet.com/news/sec/story/0,2000056024,20074799,00.htm?ref=Frst>

7

PCへの応用(1)



顔認証

出典: <http://www.g4-inc.com/event/index.html>



IRBIOマウス

虹彩認証

出典: <http://www.4media.co.jp/biz/ai/articles/070416/news107.html>

8

PCへの応用(2)



指紋認証

出典: <http://blog.get-pc.net/?cid=682692>



手のひら静脈認証

出典: <http://www.nikkei.co.jp/52/navi/05/index2.html>



指静脈認証

出典: <https://www.computerworld.jp/topics/vt/114069.html>

9

携帯電話/スマートフォンへの応用



指紋認証



サイン認証

10

自動車への応用



指静脈認証



出典: http://www.designnewsjapan.com/content/_news/2007/10/10/bp300001hoko.html

11

(2)

本人確認における バイOMETRICS認証の位置づけ

- (1) バイOMETRICS認証とは
- (2) 本人確認における
バイOMETRICS認証の位置づけ
- (3) 各種バイOMETRICS認証方式の概要紹介
- (4) バイOMETRICS認証がなぜ
- (5) バイOMETRICS認証の
ナショナルセキュリティへの応用
- (6) バイOMETRICS認証応用の将来

12

本人確認方法は、 大きく次の三つの方式に分類される

- (1) その人しか知りえない情報を知っていること
を確認することによる本人確認
→ 記憶による本人確認
- (2) その人しか持っていない等の物を持っていること
を確認することによる本人確認
→ 持物による本人確認
- (3) その人しか持ちえない生体特徴を持っていること
を確認することによる本人確認
→ 生体特徴による本人確認(バイオメトリクス認証) 13

記憶による本人確認の特徴

- * パスワード記憶方式であり簡便
- * 日常使い慣れた方式
- * 記憶できる長さ、情報量に限界
推測されやすいものになりがち
- * 多数のパスワード記憶が必要
忘失の危険大
- * 忘失対策としてのメモ→盗用の危険
- * 盗用され、悪用されても、
気がつかないことが多い 14

持物による本人確認の特徴

- * カード、携帯などによる認証方式
- * 日常的に使われ始めてきた
- * 常時携帯が必要
- * 紛失・破損・盗難の危険
- * 偽造の危険性も 15

偽造カードの被害

2007年10月 北洋銀行のキャッシュカード偽造事件

被害者 186人
被害額 141百万

ある企業の顧客情報が流出
(口座番号や生年月日)
多くの被害者が、暗証番号に生年月日！ 16

生体特徴による本人確認の特徴

- * 偽造は他の方式に比べ困難
- * 実装方法によっては、記憶も所持物も不要
- * 一度で照合できない場合もある

17

(3)

各種バイオメトリクス認証方式の概要紹介

(1)バイオメトリクス認証とは
(2)本人確認における
バイオメトリクス認証の位置づけ
(3)各種バイオメトリクス認証方式の概要紹介
(4)バイオメトリクス認証プロセス
(5)バイオメトリクス認証の
ナショナルセキュリティへの応用
(6)バイオメトリクス認証応用の将来

18

バイオメトリクス認証の 掘り所のタイプによる分類

- 外見的特徴(身体的特徴)によるもの
 - 顔
 - 網膜
 - 虹彩
 - 指紋
 - 手形
 - 手のひら静脈
 - 指静脈
 - DNA
- 行動特性(身体的特性)によるもの
 - 声紋
 - サイン
 - キーストローク

19

顔(1)



- 照合方法
 - 目や口等の代表的な顔の部品の位置を原点にして、その他の部品の位置を位置データとして2次元的に照合する方法と、何らかの計測法を用いて鼻の高さや頬の形のような3次元構造を抽出し照合する方法がある
- 精度
 - 向き、照明、髪型、サングラス、マスク等によって照合精度に影響がやすい
- 実装上の特徴
 - 顔を見て誰であるかを判断することは普段から人同士で行われており、利用者の抵抗感が少ない²⁰

顔(2)



- 実装上の特徴(続き)
 - 顔は常時露出しているため、本人が意識しなくても入力、照合可能である
- 使用される場所
 - 空港や銀行など多人数が入り出りする場所での利用が期待される
- 最近の動向
 - パソコンや携帯電話に標準でカメラが装備されており、顔照合技術の普及の下地が整ってきている

21

網膜(1)



- 照合方法
 - 眼球内部にある網膜上の血管パターンを照合する
 - 計測は、網膜に対し赤外線を直径5mm程度照射することにより行われるが、その発光強度は、自然界に存在するものより微弱であり安全とされている
- 精度
 - 識別能力は高い
 - 経年変化はほとんどない

22

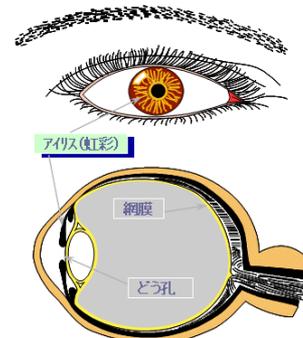
網膜(2)



- 実装上の特徴
 - センサーを覗き込み、目の奥まで光を当てなくてはならないため、利用者に抵抗感を感じさせる
 - まぶたを見開き視点を静止させるのに慣れが必要
 - システムは高価
- 使用される場所
 - 放射線施設等のハイセキュリティを要求される出入管理システムに利用される場合が多い

23

虹彩と網膜の位置関係



進化するバイオメトリクス(4) 日経BP社ウェブサイトより

24

虹彩(1)



- 照合方法
 - 虹彩(アイリス:黒目のうち瞳孔を囲む放射状の筋肉の表面にある模様)のパターンによって照合
- 精度
 - 精度は非常に高い
 - 個性が高く一生を通じて変化しない
- 実装上的特徴
 - 外部から見えやすく非接触で撮像できる

25

虹彩(2)



- 最近の動向
 - 虹彩認証の基本特許が切れ、安価でコンパクトな実装が可能で、そして精度も良い新たな虹彩認証アルゴリズムが開発された。
 - 従来の入退室セキュリティでの応用に限らず、今後、幅広く活用されることが期待される。

26

指紋(1)



- 照合方法
 - 指紋紋様には特徴点(マニューシャ)と呼ばれる固有の特徴があり、この特徴点から座標と角度を取り出してデータとして使用するのが代表的な方法である
 - 指紋画像を使って、画素毎のマッチングを行う方法もある
- 精度
 - 高精度な照合方式が確立している

27

指紋(2)



- 実装上的特徴
 - 入力センサが接触型で小型化できる
 - 皮膚の乾燥、発汗、傷、摩耗等により必要な品質のデータが得られない場合がある
 - 「指紋を取られる」ことに対する抵抗感がある
- 使用される場所
 - 社会福祉への登録など、大規模システムへの利用が進みつつある

28

声紋(1)



- 照合方法
 - 人間の声帯は個人によって大きさや形が違うので、この声帯から発せられる声の質(=声紋)も個人により違うと言われている
 - 声紋に表われる個人性情報のパターンによって照合する
- 精度
 - マイクロフォンで声を録音する時、周囲の雑音も一緒に照合してしまい照合率が悪い時がある
 - 風邪、感情起伏、声変り等の影響が大きく、照合が困難な時がある

29

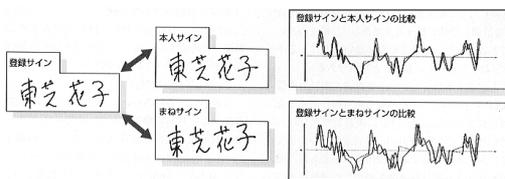
声紋(2)



- 実装上の特徴
 - 利用者の抵抗感はほとんど無い
- 使用される場所
 - 主として電話を用いるアプリケーションに使われている
- 最近の動向
 - マイクロフォンはパソコンや携帯電話、インターホンに標準で装備されているので、今後の発展が期待できる
 - NTTドコモのiモードサービスで声紋認証による相性診断や占いがヒットしている

30

サイン(1)



- 照合方法
 - 特殊なペン・タブレットを利用して筆跡や筆順、ペンの速度やペンを空中で移動しているときの軌跡、筆圧、ペンの傾き等を測定して照合を行う

31

サイン(2)



- 精度
 - 精度が他のバイオメトリクス認証方式に比べ高いとはいえない
- 実装上の特徴
 - サインすることは日常的に行われているので、利用者に受け入れやすい
 - 練習による他人の「なりすまし」が可能
- 使用される場所
 - 携帯用機器の所有者確認に使われ始めている

32

指静脈(1)

- 照合方法
 - 動脈は、酸化ヘモグロビンを体の各組織へ送り込み、酸素を供給する。静脈は、酸素を失った還元ヘモグロビンを心臓へ戻す。その血流のパターンは、個人個人によって異なる。
 - 近赤外光領域の約760nmの波長の光は、還元ヘモグロビンが吸収するため、近赤外光を当てると、静脈の血管パターンだけが暗く映る。指の透過光による静脈パターンによって照合する。
- 精度
 - 指紋、虹彩と同程度の、高い精度が期待できる。
 - 経年変化がほとんど無い。

33

指静脈(2)

- 実装上的特徴
 - 接触部分が少なく、利用者の抵抗感はほとんど無い。
- 使用される場所
 - 銀行のATM。三井住友銀行、ゆうちょ銀行、みずほ銀行など。
- 技術の特徴
 - 対応率が良い。
 - 他のバイオメトリクスに比べ偽造が困難。
 - 歴史は浅い。

34

手のひら静脈(1)

- 照合方法
 - 動脈は、酸化ヘモグロビンを体の各組織へ送り込み、酸素を供給する。静脈は、酸素を失った還元ヘモグロビンを心臓へ戻す。その血流のパターンは、個人個人によって異なる。
 - 近赤外光領域の約760nmの波長の光は、還元ヘモグロビンが吸収するため、近赤外光を当てると、静脈の血管パターンだけが暗く映る。手のひらの反射光による静脈パターンによって照合する。
- 精度
 - 指紋、虹彩と同程度の、高い精度が期待できる。
 - 経年変化がほとんど無い。

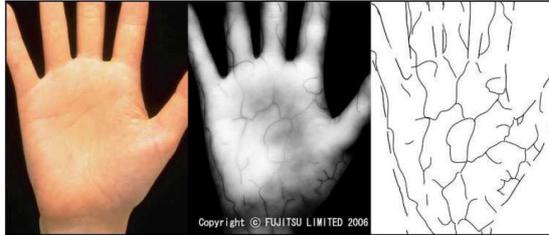
35

手のひら静脈(2)

- 実装上的特徴
 - 接触部分が無く、利用者の抵抗感はほとんど無い。
- 使用される場所
 - 銀行のATM。三菱UFJ銀行、広島銀行など。
- 技術の特徴
 - 対応率が良い。
 - 他のバイオメトリクスに比べ偽造が困難。
 - 歴史は浅い。

36

手のひら



(a) 一般のカメラで撮影した画像 (b) 赤外線カメラで撮影した画像 (c) 手のひらの輪郭および抽出した静脈パターン

37
生体認証導入・運用のためのガイドライン(IPA)より

まとめ

- バイオメトリクス認証には様々な方式がある
- 全てにおいて優れたタイプは無く、可用性、利便性や価格性能比など、実際の利用環境、システム要件などを鑑みて最適な方式を選択する必要がある

38

バイオメトリクス認証の比較

	指紋認証	顔認証	静脈認証	掌形認証	虹彩認証	網膜認証	声紋認証	署名認証
認証精度	◎	△	◎	○	◎	○	△	△
使いやすさ	◎	◎	◎	◎	○	△	◎	△
小型化	◎	○	△	△	○	△	◎	△
低価格化	◎	△	△	△	△	△	◎	○
清潔感	△	◎	△	△	◎	△	◎	△
データ漏洩	△	△	△	△	△	△	◎	◎
偽造しにくさ	○	○	○	○	◎	○	×	○
環境変化	△	△	◎	◎	◎	◎	△	△
経年変化耐性	◎	×	○	○	○	△	×	○
一瞬性双生児	◎	△	◎	△	◎	◎	△	○

(<http://www.protect-law.com/>より)⁹⁹

(4)

バイオメトリクス認証プロセス

- (1) バイオメトリクス認証とは
- (2) 本人確認におけるバイオメトリクス認証の位置づけ
- (3) 各種バイオメトリクス認証方式の概要紹介
- (4) バイオメトリクス認証のセキュリティ
- (5) バイオメトリクス認証のナショナルセキュリティへの応用
- (6) バイオメトリクス認証応用の将来

40

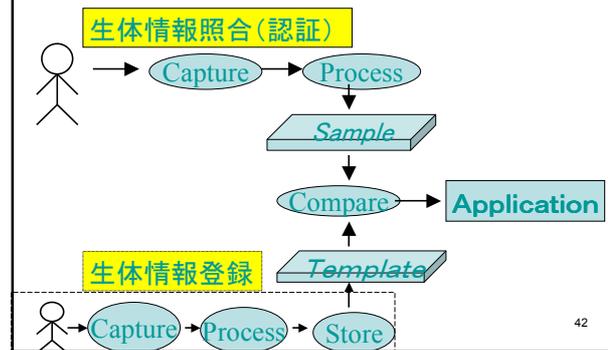
バイOMETRICS認証の 基本的な考え方

あらかじめ本人であることを確認した上で
採取した生体情報(テンプレート)
と
その場で採取した生体情報(サンプル)
を
照合することにより

その場に居る人が、あらかじめ本人であることを確
認したその人と、同一人かどうかを判定する

41

バイOMETRICS認証プロセス(1)



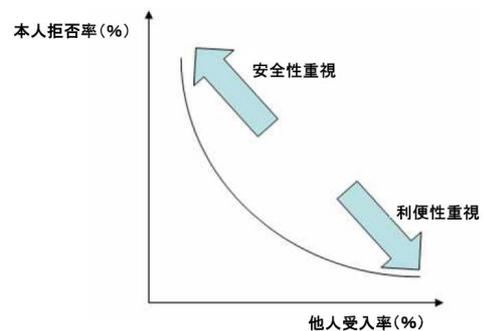
42

FARとFRR

- 本人かどうかの判定は、Compareプロセスの結果に基づき行われる
- 緩い判定基準にすると、他人を本人だと間違っ判定することもある
この確率を、FAR
(他人受入率: False Acceptance Rate)
- 厳しい判定基準にすると、本人さえも他人だと間違っ判定することもある
この確率を、FRR
(本人拒否率: False Rejection Rate)

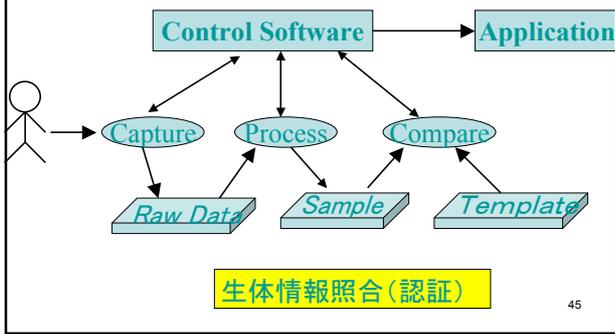
43

ROCカーブ



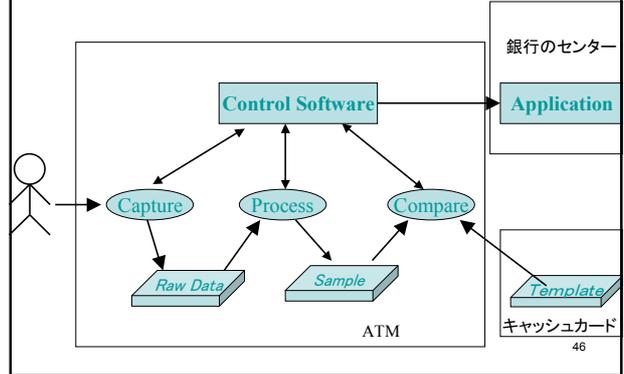
44

バイOMETRICS認証プロセス(2)



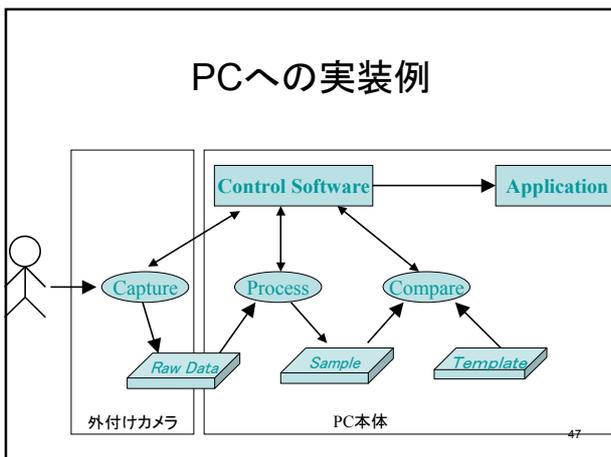
45

銀行ATMへの実装例



46

PCへの実装例



47

(5)

バイOMETRICS認証の ナショナルセキュリティへの応用

- (1) バイOMETRICS認証とは
- (2) 本人確認における
バイOMETRICS認証の位置づけ
- (3) 各種バイOMETRICS認証方式の概要紹介
- (4) バイOMETRICS認証がなぜ
- (5) バイOMETRICS認証の
ナショナルセキュリティへの応用
- (6) バイOMETRICS認証応用の将来

48

入出国管理における バイオメトリクス認証の利用

- ICAO(International Civil Aviation Organization)
国連の国際民間航空機関
2004年に、電子パスポートの基本仕様公開
必須のバイオメトリクス:顔画像
追加的に、指紋や虹彩の利用も可

49

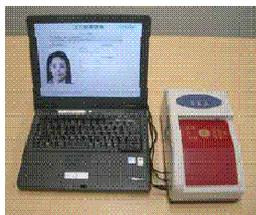
日本の入出国管理

- 2006年3月20日より、新しいパスポート(IC旅券)へ
- 顔写真を貼り替えたパスポート等を使用してもICチップに記録されている情報と照合することにより偽造を見破ることが容易
- 今後、各国の出入国審査等でICチップに記録された顔画像とその旅券を提示した人物の顔を照合する電子機器が段階的に整備されていくことにより、他人の「なりすまし」によるパスポートの不正使用防止の効果が期待
- 申請手続きは基本的に変わらず。
申請用顔写真の規格が変更
旅券発給手数料が1000円Up

50

IC旅券の読み取り

- ICチップに記録された情報の読み取り



(右) IC旅券読み取り装置
(左) ICチップから読み取った情報
(顔写真や旅券番号、名前等)を表示

(2006年の外務省資料より)

外国人の日本入国

- 2007年11月20日より、指紋採取と顔写真撮影が義務付けられた
- 入国時に指紋採取を取り入れるのは米国に続いて日本が2国目
- 成田、羽田など日本国内の27空港と126港湾すべてで適用される

52

外国人個人識別情報システム (BICS)



53

(日経ネットニュースより)

米国の入出国管理 (US-VISIT)

- 2001年9月11日の同時多発テロ対応施策の一環
- 2004年9月30日より、入国審査時に両手の人差し指2本の指紋採取とデジカメラによる顔写真の撮影されることに
- 2008年末には、全ての地点での入国審査時に、指紋採取・顔写真撮影が、実施される予定
- 2007年11月29日より、ワシントン・ダレス空港にて、10本の指紋採取が開始された。(現在は全ての空港で採取されている)
- 2009年1月12日より、電子渡航認証システムESTAを通じての事前の渡航認証を義務付け
- 2009年7月2日より、アトランタ、デトロイトの二つの空港で、出国時のバイオメトリクス利用のトライアルが開始された。今年中には、全空港でバイオメトリクスを利用した新たな出国手続きが導入される予定。
- [US-VISIT説明ビデオ\(3分余\)](#)

54

アラブ首長国連邦(UAE)の入国審査

- 2001年より17箇所の全ての国境審査にて
外国人の入国審査に虹彩認証を採用
- 80%が海外の人の入国
- ブラックリスト 50万人のDB
- 1日7000人の海外からの入国
- 危険人物の発見例
DBのデータに合致
ブラックリストに登録されていた
次のフライトで、自国へ送還された

[映像\(約3分\)](#)

55

(6)

バイオメトリクス認証応用の将来

- (1) バイオメトリクス認証とは
- (2) 本人確認における
バイオメトリクス認証の位置づけ
- (3) 各種バイオメトリクス認証方式の概要紹介
- (4) バイオメトリクス認証がなぜ
- (5) バイオメトリクス認証の
ナショナルセキュリティへの応用
- (6) バイオメトリクス認証応用の将来

56

開発中(検討中)の応用例

指紋認証機能搭載ICカード

[NEDO「イノベーション推進事業」](#)

動きながらのバイOMETRICS認証

[Iris on the Move\(5分10秒\)](#)

バイOMETRICSによる将来の認証・決済基盤

[Okkoidビデオ\(6分余\)](#)

< 本日の内容 > バイOMETRICS認証

- (1) バイOMETRICS認証とは
- (2) 本人確認における
バイOMETRICS認証の位置づけ
- (3) 各種バイOMETRICS認証方式の概要紹介
- (4) バイOMETRICS認証プロセス
- (5) バイOMETRICS認証の
ナショナルセキュリティへの応用
- (6) バイOMETRICS認証応用の将来

58

終りに

- バイOMETRICSは確実に皆さんの生活の場へ浸透しつつある。
- 一方、まだまだ解決すべき課題も多く、研究・技術開発テーマの宝庫であり、
- また、先駆的応用は始まりつつあるも、新たな応用、事業創出の宝庫でもある。
- 本講義が、それぞれの立場で、バイOMETRICS分野への対応を検討するきっかけになれば幸いです。

59

レポート課題

次の三種の本人確認方法のそれぞれについて、バイOMETRICS認証に基づく本人確認方法かどうかを判定し、かつ、その理由を述べなさい。

①あらかじめ本人確認した上で本人が定めたパスワードをシステムへ登録しておく。本人が定めたパスワードをその場で音声で答えさせ、音声認識により抽出した文字列と登録されているパスワードとの照合により、その場に居る人が本人かどうかを判定する。

②あらかじめ本人確認した上でシステムへ登録した本人の指紋データと同じデータを本人のICカードに格納しておく。本人のICカードをその場で提示させ、そのICカードに格納されている指紋データと登録されている指紋データとの照合により、その場に居る人が本人かどうかを判定する。

③あらかじめ本人確認した上で本人の虹彩データをシステムへ登録しておく。本人の虹彩データをその場で採取し、その虹彩データと登録しておいた虹彩データとの照合により、その場に居る人が本人かどうかを判定する。

60

レポート課題

バイオメトリクス認証を利用している方はAを、
未だ利用したことが無い方はBを、選択してください。

A: バイオメトリクス認証を利用している方

問題2: 利用場面は？

問題3: 利用しているバイオメトリクス認証は？

問題4: バイオメトリクス認証を利用して、
便利な点、不便な点は？(理由を含め)

B: バイオメトリクス認証を利用していない方

問題2: 利用すると便利になりそうな場面は？

問題3: どのようなバイオメトリクス認証が適している？

問題4: 便利になると思う理由は？(具体的に)

終

62

問題1

バイオメトリクス認証はどれか。

- ア 個人の指紋や虹彩などの特徴に基づく認証
- イ 個人の知識に基づく認証
- ウ 個人のパターン認識能力に基づく認証
- エ 個人の問題解決能力に基づく認証

63

問題2

生体認証システムを導入するときに考慮すべき点として、最も適切なものはどれか。

- ア システムを誤作動させるデータを無害化する機能をもつライブラリを使用する。
- イ パターンファイルの頻繁な更新だけでなく、ヒューリスティックなど別の手段を組み合わせる。
- ウ 本人のデジタル証明書を信頼できる第三者機関に発行してもらう。
- エ 本人を誤って拒否する確率と他人を誤って許可する確率の双方を勘案して装置を調整する。

64

問題3

バイオメトリクス認証システムの判定しきい値を変化させるとき、FRR (本人拒否率) と FAR (他人受入率) との関係はどれか。

- ア FRR と FAR は独立している。
- イ FRR を減少させると、FAR は減少する。
- ウ FRR を減少させると、FAR は増大する。
- エ FRR を増大させると、FAR は増大する。

65

記述問題(アンケート)

問題1: バイオメトリクス認証を利用している方はAを、未だ利用したことが無い方はBを記入してください。

A: バイオメトリクス認証を利用している方

問題2: 利用場面は？

問題3: 利用しているバイオメトリクス認証は？

問題4: バイオメトリクス認証を利用して、便利な点、不便な点は？(理由を含め)

B: バイオメトリクス認証を利用していない方

問題2: 利用すると便利になりそうな場面は？

問題3: どのようなバイオメトリクス認証が適している？

問題4: 便利になると思う理由は？(具体的に)

正解

- 問題1 ア
- 問題2 エ
- 問題3 ウ

67